A weak equivalence between shifts of finite type

Marie-Pierre Béal, Dominique Perrin

A weak equivalence between shifts of finite type

MARIE-PIERRE BÉAL
Institut Gaspard-Monge,
Université de Marne-la-Vallée
http://www-igm.univ-mlv.fr/~beal

DOMINIQUE-PERRIN
Institut Gaspard Monge,
Université de Marne-la-Vallée
http://www-igm.univ-mlv.fr/~perrin

September 27, 2001

Abstract

We introduce the following notion of weak equivalence between shifts of finite type. Two shifts of finite type S and T are equivalent if and only if there are finite alphabets A and B and sliding block maps f from $A^{\mathbb{Z}}$ to $B^{\mathbb{Z}}$ and g from $B^{\mathbb{Z}}$ to $A^{\mathbb{Z}}$ such that $S \subset A^{\mathbb{Z}}$, $T \subset B^{\mathbb{Z}}$, $S = f^{-1}(T)$ and $T = g^{-1}(S)$. We give a necessary condition for this equivalence and we show how to decide the equivalence when the shifts are given by finite circular codes.

1 Introduction

In this paper, we introduce a notion of weak equivalence between shifts of finite type. Shifts of finite type can be seen both from the point of view of the mathematical theory of symbolic dynamics and from the point of view of finite automata theory. Some practical applications from these areas have been found in the field of coding into constrained channels. From the automata theory point of view that we adopt, a shift of finite type is the set of bi-infinite words recognized by a finite local automaton. An automaton is local if it does not admit two distinct equally labeled cycles. The automata are such that all states are both initial and final. The labeling is in a finite alphabet. When one can choose an automaton such that all labels of edges are distinct, the shift is called an edge shift.

Several notions of equivalence have been studied, in order to classify the shifts of finite type and other more general symbolic dynamical systems, like shift equivalence and strong shift equivalence (see [6]). The strong shift equivalence is the conjugacy or isomorphism between two systems. An isomorphism is a bijective continuous map that commutes with the shift operation on bi-infinite words. The decidability of strong shift equivalence between shifts of finite type is still an open question. Some invariants have been found but none of them is a characteristic one.

The notion of weak equivalence that we introduce here is much weaker than the previous ones. Two shifts of finite type S and T are are equivalent if and only if there are finite alphabets A and B and sliding block maps f from $A^{\mathbb{Z}}$ to $B^{\mathbb{Z}}$ and g from $B^{\mathbb{Z}}$ to $A^{\mathbb{Z}}$ such that $S \subset A^{\mathbb{Z}}$, $T \subset B^{\mathbb{Z}}$, $S = f^{-1}(T)$ and $T = g^{-1}(S)$. The topological entropy for example is no more an invariant for this equivalence relation. We prove that the weak equivalence is decidable for a subclass of edge shifts called the flower edge shifts, that is the shifts that are generated by a finite circular code, or, equivalently, the shifts recognized by a flower automaton whose edges have distinct labels. An equivalence class for this relation is characterized by the signature of the flower edge shift which is given by the length sequence of a minimal generating system of the ideal of $\mathbb{N}$ of periods of words of the flower edge shift.

For more general edge shifts, we give a trivial necessary condition for their equivalence but the question of decidability of their equivalence is open. At the end of the paper, we give an example of a flower edge shift which is weakly equivalent to a non flower one.

2 Definitions and background

We first recall some basic definitions about subshifts and sliding block maps. We refer to [5], [6], or [3], [2] for more details about these notions coming from symbolic dynamics.

If A is a finite alphabet, we consider the set $A^{\mathbb{Z}}$ of two-sided infinite words as a topological space with respect to the usual product topology. The *shift* transformation σ acts on $A^{\mathbb{Z}}$ bijectively. It associates to $x \in A^{\mathbb{Z}}$ the element $y = \sigma(x) \in A^{\mathbb{Z}}$ defined for $n \in \mathbb{Z}$ by

$$y_n = x_{n+1},$$

and obtained by shifting all symbols one place left. A *symbolic dynamical system* or *subshift* is a subset S of $A^{\mathbb{Z}}$ which is both topologically closed and shift-invariant, i.e. such that $\sigma(S) = S$.

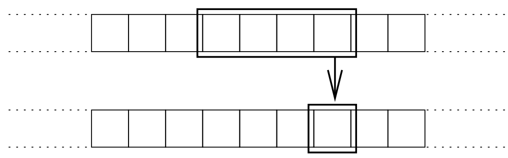

Figure 1: A sliding block map

Let G be a directed graph with E as its set of edges. We actually use multigraphs instead of ordinary graphs in order to be able to have several distinct edges with the same origin and end. We shall always say "graph" for "directed multigraph". Let S_G be the subset of $E^{\mathbb{Z}}$ formed by all bi-infinite paths in G. It is clear that S_G is a subshift called the *edge shift* on G. Indeed S_G is closed and shift invariant by definition.

Let $\mathcal{A} = (Q, E)$ be a *finite automaton* on an alphabet A given by a finite set Q of states and a set $E \subset Q \times A \times Q$ of edges, all states being both initial and final. The set of all labels $\cdots a_{-1}a_0a_1\cdots$ of the bi-infinite paths

$$\cdots p_{-1} \xrightarrow{a_{-1}} p_0 \xrightarrow{a_0} p_1 \cdots$$

is a subshift S. We say that S is the subshift *recognized* by the automaton $\mathcal{A}$. A subshift obtained in this way is called a *sofic shift*. It is *transitive* iff it can be recognized by an automaton with a strongly connected underlying graph.

A *shift of finite type* is a subshift which is made of all infinite words avoiding a given *finite* set of blocks. It is a sofic shift. Any edge shift is of finite type and is characterized by a finite list of forbidden blocks of length 2. An allowed block is a finite word that is subblock of at least one bi-infinite word of the shift.

Let $S \subset A^{\mathbb{Z}}$ and $T \subset B^{\mathbb{Z}}$ be two subshifts and let $k \geq 1$ be an integer. A function $f : S \to T$ is said to be a *k-sliding block map* if there is a function $\overline{f} : A^k \to B$ and an integer $a \in \mathbb{Z}$, called the anticipation, such that for all $x \in S$ the word $y = f(x)$ is defined for $n \in \mathbb{Z}$ by

$$y_{n-a} = \overline{f}(x_{n-(k-1)} \cdots x_{n-1}x_n) \tag{1}$$

Thus the value of a symbol in the image is a function of the symbols contained in a window of length k above it, called a *sliding window* (represented on Figure 1 in the case $a = 0$). It is known (see for instance [6]) that sliding block maps are exactly the maps f that are continuous and commute with the shifts, i.e. such that $f\sigma = \sigma f$.

An isomorphism or a *conjugacy* is a bijective sliding block map. The inverse is also a sliding block map. Two isomorphic shifts are also said to be conjugate or strong shift-equivalent. Any shift of finite type is isomorphic to an edge shift.

A finite non empty word x is said to be *primitive* if $x = u^n$, where $n \geq 1$ and u is a word, implies $n = 1$ and $u = x$. Let x be a finite primitive word. The bi-infinite word y obtained by infinite concatenations of x left and right and such $y_0 \dots y_{|x|-1} = x$ is denoted by $\bar{x}$.

$$\bar{x} = \dots xxxx.xxxx \dots$$

We denote by $(x)^{\mathbb{Z}}$ the set $\{\sigma^n(\bar{x}) \mid n \in \mathbb{Z}\}$, that is the orbit of $\bar{x}$.

We consider a finite set X of n finite words such that all letters of all words are distinct. We denote by $F(X^*)$ the set of finite factors of concatenations of words of X. We call S_X the shift of finite type defined as the bi-infinite words whose finite factors belong to $F(X^*)$. The shift S_X is an edge shift recognized by an automaton constructed with n cycles around one central state, each cycle being labeled by one word of X. Such a shift is called the *flower edge shift* $(l_1, l_2, \dots, l_n)$, where $(l_1, l_2, \dots, l_n)$ is the length distribution of the set X. In Figure 2 is represented on the left the flower edge shift $(2, 3, 5)$ by an automaton recognizing S_X, where $X = \{ab, cde, fghij\}$. On the right part of the figure the same automaton is represented by a labeled graph such that each edge labeled i represents a path of length i with same origin and end. The labeling is omitted in this last compact representation. Note that flower edge shifts are transitive

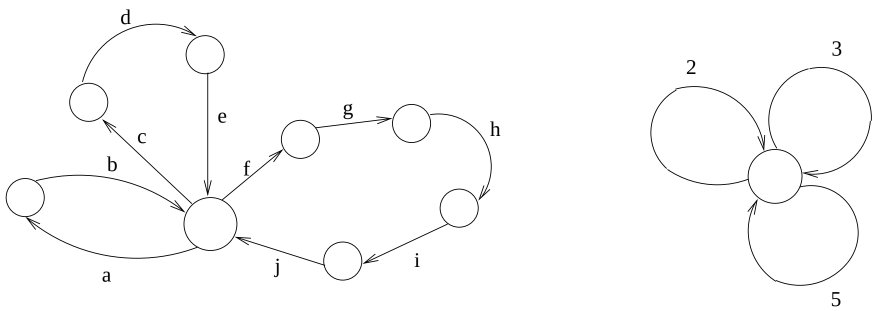

Figure 2: The flower edge shift $(2, 3, 5)$

shifts.

Let A be an alphabet. A subset C of A^+ is said to be a *circular code* (see [4]) if for all $n, m \geq 1$ and $x_1, x_2, \dots, x_n \in C$, $y_1, y_2, \dots, y_m \in C$, and

$p \in A^*$ and $s \in A^+$, the equalities

$$\begin{aligned} sx_2 \ldots x_n p &= y_1 y_2 \ldots y_m \\ x_1 &= ps \end{aligned}$$

imply

$$n = m, p = \epsilon, \text{ and } x_i = y_i \ (1 \leq i \leq n)$$

Let C be a finite set of distinct words that is a circular code. The shift S_C defined as the bi-infinite words whose finite factors belong to $F(C^*)$ is a shift of finite type which is strong shift equivalent to the flower edge shift defined by a code X which has the same length distribution (see for instance [2]). This allows us to work in Section 4 with flower edge shifts and to omit the labeling on these graphs. We consider that each edge has a label which is distinct from the others.

3 The weak equivalence

We define a notion of weak equivalence between subshifts. This notion is much weaker than the notions of strong shift-equivalence and shift-equivalence (see [6] for these notions).

Definition Let S and T be two symbolic subshifts. We note $S \to T$ or $T \prec S$ if and only if there are finite alphabets A and B and a sliding block map from $A^{\mathbb{Z}}$ to $B^{\mathbb{Z}}$ such that $S \subset A^{\mathbb{Z}}$, $T \subset B^{\mathbb{Z}}$ and $S = f^{-1}(T)$. We say that S and T are *weakly equivalent*, and we note it $S \sim T$ if and only if $S \to T$ and $T \to S$.

We can remark that the relation $\to$ is reflexive and transitive. It is a partial order. Note that if $S = f^{-1}(T)$, then $f(S) \subset T$. Two strong shift-equivalent (or isomorphic) subshifts are of course weakly equivalent. This allows us to consider shifts of finite type that are always edge shifts, i.e. that are recognized by finite automata whose edges all have distinct labels, since every shift of finite type is isomorphic to an edge shift. It is also known that the inverse image of a shift of type by a sliding block map is a shift of finite type. Then a shift of finite type cannot be weakly equivalent to a subshift which is not of finite type. As we shall see later, the topological entropy is not an invariant of weak equivalence.

Let u be a (bi-infinite) word of $A^{\mathbb{Z}}$. We say that a positive integer p is a *period* of u iff $\sigma^p(u) = u$. The word u is said to be periodic when such an integer exists. We call *the period of* u the smallest integer with this property. The period of u divides all other periods of u. Let f be a sliding block map from $A^{\mathbb{Z}}$ to $B^{\mathbb{Z}}$. Since $f\sigma = \sigma f$, if u is a periodic word, $f(u)$ also and the period of $f(u)$ divides the period of u. From this we get the following proposition.

Proposition 1 *Let S and T be two symbolic subshifts with $S \to T$. If S has a word of period n, then T has a word of period m dividing n.*

Proposition 2 *Let T be a symbolic subshift that has a word of period p. Let x be a finite primitive word of length multiple of p. Then $(x)^{\mathbb{Z}} \to T$.*

Proof: Let us assume that T is a subshift of $B^{\mathbb{Z}}$, where B is a finite alphabet. Let $u = (u_i)_{i \in \mathbb{Z}}$ be a bi-infinite word of period p of T. Thus for each integer n, we have $u_{n+p} = u_n$. Let $x = x_1 x_2 \ldots x_{kp}$ be a primitive word of A^*, where k is a positive integer and A is a finite alphabet. We define a kp-sliding block map f with a null anticipation from $A^{\mathbb{Z}}$ to $(B \cup \{\$\})^{\mathbb{Z}}$, where \$ does not belong to B, by defining the image by $\bar{f}$ of any block of length kp as follows. We map each block $(x_i, x_{i+1}, \cdots, x_{kp}, x_1, x_2, \ldots, x_{i-1})$ to u_{i-1}, and any other block to \$. It is then easy to verify that $f^{-1}(T) = (x)^{\mathbb{Z}}$. $\Box$

Proposition 3 *Let S be a transitive shift of finite type such that the g.c.d of the periods of periodic words of S is equal to d. Let x be a primitive finite word of length dividing d. Then $S \to (x)^{\mathbb{Z}}$.*

Proof: Without loss of generality, we assume that S is an edge shift, recognized by a finite automaton $\mathcal{A}$ that has a strongly connected graph and edges with distinct labels in an alphabet A. The g.c.d. of the lengths of cycles of the graph of the automaton is equal to g.c.d., denoted by d, of periods of periodic words of S.

Let $x = x_0 x_1 \ldots x_{k-1}$ be a word of length k dividing d on an alphabet B. Since the g.c.d. of the lengths of the cycles of the graph of $\mathcal{A}$ is d, one can label each state of $\mathcal{A}$ with a number in $\mathbb{Z}/k\mathbb{Z}$, in such a way that each path of length l goes from a state labeled i to a state labeled $i + l \pmod{k}$.

We define a two block map f from $A^{\mathbb{Z}}$ to $(B \cup \{\$\})^{\mathbb{Z}}$, by defining the image of a block of two letters of A by $\bar{f}$. Let ab be a block of letters of length two such that a is the label of an edge ending in a state s labeled by $(i-1) \bmod k$ and b the label of an edge starting at s and ending in a state labeled by $i \bmod k$, we define $\bar{f}(a, b)$ as x_i. Note that b is the label of an edge that can follow the unique edge labeled by a in the graph. One maps other two-blocks to \$ by $\bar{f}$. We define f from $\bar{f}$ with a null anticipation.

If u is a word of S, we get $f(u) \subset (x_0x_1 \dots x_{k-1})^{\mathbb{Z}} = (x)^{\mathbb{Z}}$. Conversely $f^{-1}((x)^{\mathbb{Z}})$ is a set of bi-infinite words such that any subblock ab of length two is an allowed block of S, that is b is the label of an edge that can follow the unique edge labeled a in the graph. Then $f^{-1}((x)^{\mathbb{Z}}) \subset S$. $\square$

As a consequence of the two previous propositions, we get the following one.

Proposition 4 *Let S be a transitive shift of finite type which has a periodic word whose period divides all other periods of words of S, then $S \sim (x)^{\mathbb{Z}}$, where x is a (primitive) finite word.*

Proof: Let p be the period of a periodic word of smallest period, which is also the g.c.d of periods of words of S. Let x be a finite primitive word of length p. By Proposition 2, $S \to (x)^{\mathbb{Z}}$. By Proposition 3, $(x)^{\mathbb{Z}} \to S$. Hence $S \sim (x)^{\mathbb{Z}}$. $\square$

4 Decidability of weak equivalence of flower edge shifts

In this section, we only consider flower edge shifts. These shifts are completely determined by the length distribution of the words of a finite set of words X. Let S_X be such a shift, we denote by $s = (s_1, s_2, ..., s_n)$ the length distribution of X. We can moreover assume that $s_1 \leq s_2 \leq \cdots \leq s_n$. We denote by $< s >$ the ideal $s_1\mathbb{N} + s_2\mathbb{N} + \cdots s_n\mathbb{N}$ of $\mathbb{N}$. It is called the *spectrum* of s and s is a generating system of $< s >$ as ideal of $\mathbb{N}$.

Proposition 5 *There is a unique (up to a permutation) minimal generating system of $< s >$.*

Proof: Let $s = (s_1, s_2, ..., s_n)$ and $t = (t_1, t_2, ..., t_m)$ be two minimal generating systems of $< s >$, with $s_1 \leq s_2 \leq \cdots \leq s_n$ and $t_1 \leq t_2 \leq \cdots \leq t_m$. Since $< s > \subset < t >$, we get

$$s_1 = t_i a_i + \cdots t_m a_m, \text{ with } a_i \neq 0, a_i \in \mathbb{N}.$$

This implies that $t_i \leq s_1$, and thus $t_1 \leq s_1$. Conversely we get $s_1 \leq t_1$ and then $s_1 = t_1$.

Let us now suppose that $< (s_2, ..., s_n) > \neq < (t_2, ..., t_m) >$ and $s_2 \leq t_2$. If s_2 belongs to $< (t_2, ..., t_m) >$, we get $t_2 \leq s_2$, $s_2 = t_2$. If not, s_2 does not belong to $< (t_2, ..., t_m) >$ and $s_2 \leq t_2 \leq \cdots \leq t_m$. Then

$$s_2 = s_1 b_1 + t_2 b_2 + \cdots + t_m b_m \text{ with } b_1 \neq 0, b_i \in \mathbb{N}.$$

Since $s_2 \leq t_2 \leq \cdots \leq t_m$, we get $b_2 = \cdots = b_m = 0$. This implies that $s = (s_1, s_2, ..., s_n)$ is not minimal.

We now have $s_1 = t_1$ and $s_2 = t_2$. We iterate the process with the same arguments by assuming for instance that $s_3 \leq t_3$. If s_3 does not belong to $< (t_2, \ldots, t_m) >$,

$$s_3 = s_1 b_1 + s_2 b_2 + t_3 b_3 + \cdots + t_m b_m$$

with b_1 or b_2 non null. Since $s_3 \leq t_3$, we get $b_3 = \cdots = b_m = 0$ and s is again non minimal since $s_3 = s_1 b_1 + s_2 b_2$. We iterate the process for the remaining indices and get the result since both generating systems are minimal. $\Box$

We can remark that even if the minimal generating system is unique, the decomposition in a nonnegative integral linear combination of elements of the system is not.

The minimal generating system of the system generated by the length distribution of a finite set X is called the *signature* of X or the signature of the shift S_X.

We now prove that the weak equivalence for flower edge shifts is decidable. This is a consequence of the two following propositions.

Proposition 6 *Let $S = S_X$ and $T = T_Y$ be two flower edge shifts where X and Y have respectively the length distributions $s = (s_1, ..., s_n)$ and $t = (t_1, ..., t_m)$. Then $S \sim T$ if and only if $< s >=< t >$.*

Proof: In one direction, if $< s >=< t >$, we have $s_{min} = t_{min}$, where s_{min} (resp. t_{min}) denotes the minimal generating system extracted from s (resp. t). A subcode X_1 of X (resp. Y_1 of Y) has s_{min} (resp. t_{min}) as length distribution. We define a 2-sliding block map f from S to T with a null anticipation from $\bar{f}$ that maps each allowed block ab of length two of S, where b is the letter of index i of a word of X_1, to the letter of index i of the word of same length of Y_1. Let now $u = u_1 \ldots u_k$ be a word of X which does not belong to X_1. Then the length of u is the sum of the lengths of words $z_1, \ldots, z_i$ of Y (the words z_i are not supposed to be distinct). This allows us to define a mapping g which associates to each letter of u a letter of $z_1, \ldots, z_i$ such that $g(u)$ is an allowed block of T. Wew then define $\bar{f}$ for any allowed block of length two ab of S where b is a letter of u as $g(b)$. If ab is not an allowed block of S, we define $\bar{f}(ab) = \$$, where $\$$ is not a symbol of T. We get $S = f^{-1}(T)$. By symmetry, $S \sim T$.

In the other direction, we consider that $S \sim T$. By Proposition 1, we get that if S has a word of period k, then T has a word of period dividing

k. Without loss of generality, we can assume that s and t are minimal generating systems of $< s >$ and $< t >$. Since the set $< s >$ is the set of values of periods of words of S, we get that there is a matrix A with nonnegative integral coefficients such that

$$s.A \;/\; t$$

(the dividing property is satisfied coefficients by coefficients). There is also a nonnegative integral matrix B such that

$$t.B \;/\; s.$$

We get

$$s.AB \;/\; s.$$

We obtain

$$< s > \subset < s.AB > \subset < s.A > \subset < s >$$

Since $s.A \;/\; t$, we also have:

$$< t > \subset < s.A > = < s > .$$

Symmetrically, we get $< s > = < t >$. $\square$

Proposition 7 *Let $S = S_X$ and $T = T_Y$ be two flower edge shifts where X and Y have respectively the length distributions $s = (s_1, ..., s_n)$ and $t = (t_1, ..., t_m)$. It is decidable if $< s > = < t >$.*

Proof: If $< s > = < t >$, then s_{min} is equal to t_{min}, where s_{min} is the minimal generating system of the spectrum of X. The computation of s_{min} from s can be done as follows. It can be reduced to the problem of checking whether s_1 can be removed from $< s_2, \ldots, s_n >$, that is whether s_1 belongs to $< s_2, \ldots, s_n >$. This is computable since the coefficients are nonnegative integers and there only a finite number of values to check. $\square$

Example The flower edge shifts $(2, 3)$, $(2, 3, 3)$, $(2, 3, 5)$ are all weakly equivalent since $5 = 2+3$. Remark that they all have different topological entropy. They all have the same signature $(2, 3)$.

Corollary 1 *Let S and T be two flower edge shifts. It is decidable whether $S \sim T$.*

In the more general case of edge shifts that are not flower edge shifts, we have the partial following result. Let G be a graph. We call the *spectrum* of the lengths of the cycles of G the sequence $s = (s_1, s_2, \ldots, s_n)$ where $s_i = 1$ if there is a cycle of length i and $s_i = 0$ if not.

Proposition 8 *Let S and T be two edge shifts given by two finite graphs G and H. It is decidable whether the spectrum of the lengths of cycles of the two graphs are equal.*

Proof: Let A (resp. B) be the adjacency matrix of G (resp. H). The coefficient of index ij of the adjacency matrix is 1 if there is at least one edge from i to j in the graph. The coefficients of A and B can be seen in the boolean ring. Checking whether the spectrum of the lengths of cycles of the two graphs are equal is equivalent to checking whether $tr(A^n) = tr(B^n)$ for each positive integer n, where tr denotes the trace of a matrix. For any matrix A in the boolean ring, there are two positive indices $i < j$ such that $A^i = A^j$. There is then a finite number of equalities to check. This proves the decidability of the problem. $\square$

The condition given in the statement of Proposition 8 is a necessary condition for weak equivalence. But we don't know if it is a sufficient condition. Moreover, a flower edge shift can be weakly equivalent to a non flower one as it is shown in the following example.

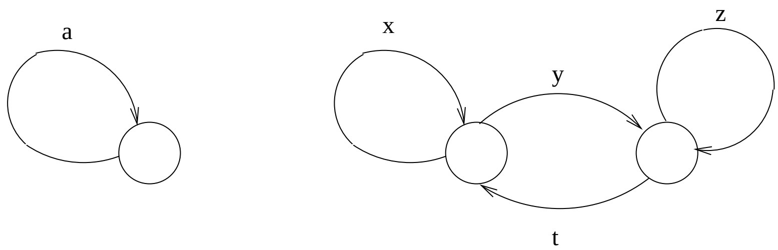

Figure 3: Two weakly equivalent edge shifts: S (on the left) and T (on the right)

Example The two edge shifts $S \subset \{a\}^{\mathbb{Z}}$ and $T \subset \{x, y, z, t\}^{\mathbb{Z}}$ given by the graphs of Figure 3 are weakly equivalent. Indeed, the graph of the edge shift $S = (1)$ is a subgraph of the other edge shift T. Thus we have $S \to T$ since we can take the one block map from S to T that maps the letter a to the letter x. In the other direction, a 2-sliding block map with a null anticipation f from T to S is defined by $\bar{f}(xx) = \bar{f}(xy) = \bar{f}(yz) = \bar{f}(yt) = \bar{f}(zz) = \bar{f}(zt) = \bar{f}(tx) = \bar{f}(ty) = a$, and by $\bar{f}(u) = \$$ for any forbidden block u of length two of T. Then $T = f^{-1}(S)$. The equivalence $S \sim T$ is also a consequence of Proposition 4.

References

[1] Adler, R. L., Coppersmith, D., and Hassner, M. Algorithms for sliding block codes. *IEEE Trans. Inform. Theory IT-29*, 1 (1983), 5–22.

[2] Béal, M.-P. *Codage Symbolique.* Masson, Paris, 1993.

[3] Béal, M.-P., and Perrin, D. Symbolic dynamics and finite automata. In *Handbook of Formal Languages*, G. Rozenberg and A. Salomaa, Eds., vol. 2. Springer-Verlag, Berlin and New York, 1997, ch. 10.

[4] Berstel, J., and Perrin, D. *Theory of Codes.* Academic Press, New York, 1985. http://www-igm.univ-mlv.fr/~berstel/LivreCodes/Codes.html.

[5] Kitchens, B. P. *Symbolic Dynamics: one-sided, two-sided and countable state Markov shifts.* Springer-Verlag, 1997.

[6] Lind, D. A., and Marcus, B. H. *An Introduction to Symbolic Dynamics and Coding.* Cambridge University Press, 1995.

[7] Perrin, D. Finite automata. In *Handbook of Theoretical Computer Science*, J. V. Leeuven, Ed., vol. B. Elsevier, Amsterdam, 1990, ch. 1.